UNITED STATES DISTRICT COURT

for the

District of Massachusetts

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Western Digital WD800 hard drive S/N WCAM93136842 (Item 5)	)	Case No. 18-mj-6006-MPK

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the _____ District of Massachusetts
(identify the person or describe the property to be searched and give its location):

Western Digital WD800 hard drive S/N WCAM93136842 (Item 5); as further described on Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B

YOU ARE COMMANDED to execute this warrant on or before January 20, 2018 *(not to exceed 14 days)*
☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to U.S. Magistrate Judge M. Page Kelley.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: January 10, 2018 1:43 p.m. Kelley
Judge's signature

City and state: Boston, Massachusetts U.S. Magistrate Judge M. Page Kelley
Printed name and title

Return

Case No.: 18-mj-6006-MPK	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

Attachment A

MSi Laptop computer, S/N K1701N0052393 (Item 2a);

LG black in color cell phone with cracked screen (Item 2b);

Samsung white in color cell phone with cracked screen (Item 2c);

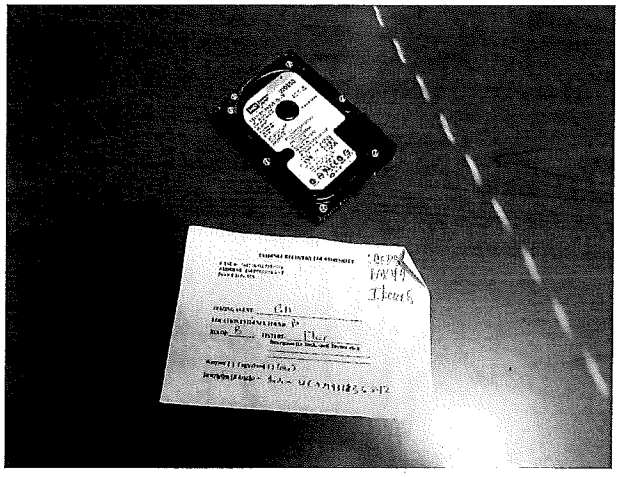
Samsung black in color cell phone with a cracked screen (Item 2d)

Motorola black in color cell phone (Item 2e)

Motorola black in color cell phone (Item 2f)

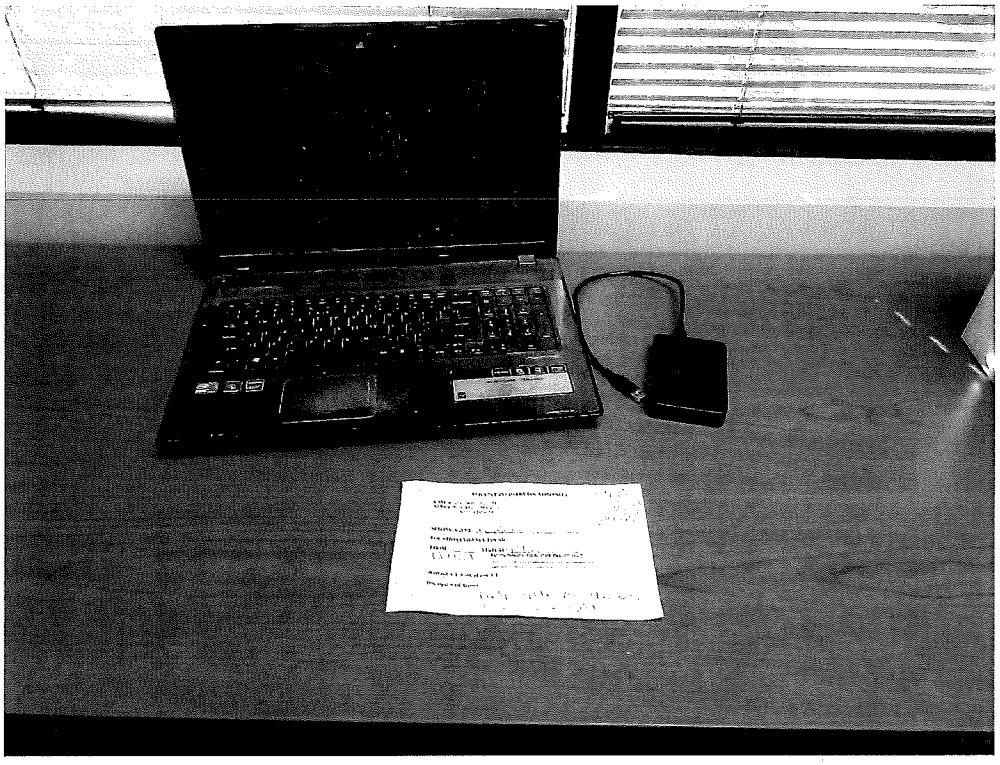
See photograph below:

Western Digital WD800 hard drive S/N WCAM93136842 (Item 5). See photograph below:



Acer laptop computer, S/N LXRCB02010047026492000 (Item 7a)

Western Digital hard drive S/N WX21A82L4583 (Item 7b). See photograph below:



Attachment B

All evidence of the commission of criminal offenses in violation of the introduction into interstate commerce of misbranded and unapproved new drugs, in violation of 21 U.S.C. §§ 331(a), 331(d), and 333(a); conspiracy to introduce into interstate commerce misbranded and unapproved new drugs, in violation of 18 U.S.C. § 371; and manufacturing and distributing controlled substances, in violation of 21 U.S.C. § 841(a)(1), contraband, the fruits of a crime, things criminally possessed, and/or property designed or intended for or which is or has been used as the means of committing a criminal offense, in violation of the foregoing statutes, and records which would show the disposition of proceeds of these offenses, including but not limited to he following.

1. Banking records for Daniel McCarron relating to domestic bank accounts or foreign bank accounts, including but not limited to, bank statements, passbooks, account access cards, checkbooks, cancelled checks, check registers, cashier checks, wire transfer requests, confirmation slips, credit card statement, debit card statements, advice memos, ledgers, money drafts, money order and cashier's check receipts, bank checks, signature cards, account holder instructions, currency exchange records, and/or any other items evidencing the obtaining, secreting, transfer, and/or concealment of assets and the obtaining, secreting, transfer, concealment, and/or expenditure of money.

2. Any and all digital books and records, including but not limited to inventories, accounting journals, correspondence, communication, reports, financial statements, balance sheets, wire transfer instruction, loans, corporate tax returns, invoices, cash register sales and/or receipts, billing statement, medical records, subscription agreements, provider agreements, physician agreements, sales materials, investor information, training materials, policy manuals, and any other documents or business records related to the establishment and/or operation of any business affiliated with Danial McCarron.

3. Any and all pharmacy/pharmaceutical records of returned, expired, and/or waste medications as well as the dispensing of returned, expired and/ or waste medication, including but not limited to, communication, correspondence, medication lists, inventories, prescriptions, prescription labels, destruction/disposal records, inventories, daily logs, audits, reverse distributor lists and reverse distributor invoices reflecting returns of pharmaceuticals and/or purchase histories.

4. Any and all pharmacy/pharmaceutical records, including but not limited to, prior authorization logs, dispensing records, prescription orders/delivery records, purchasing records, distributor audits, call in medication request/orders, unclaimed medication records, refill request forms, destruction/disposal records, expired drug lists, reverse distributer records, owed slips, compounding logs and records, medication error reports, audit and compliance reports,

prescription log reports, prescription fill/refill summary, delivery logs, signature logs, or documents tracking the refilling of prescriptions and claims for the same.

5. Any and all customer profiles.

6. Any and all drug recall alerts.

7. Any and all pharmacy/pharmaceutical records reflecting medications not distributed including but not limited to "owed slips", customer lists, adjustments, insurance billings, prescriptions and prescription labels.

8. U.S. Mail records, UPS records, and any other commercial parcel carrier receipts related to the receipt, mailing, and sell or trade of medications.

9. All FDA policies, correspondence, transmittal, program memoranda, instructions and other guidelines.

10. All pharmacy manuals or similar instructional manuals, as well as employee handbooks or manuals.

11. Any and all records of employees, including but not limited to personnel files, contracts, payroll, licensing information, training and education, employee handbooks or manuals, performance appraisals, awards, discipline or recognition.

12. Correspondence from and to the customers and correspondence to and from the suppliers of components to the sell or trade of medications or documents clarifying those prescriptions drugs or steroids that were sold.

13. Any cellular telephones and associated telephone bills. With regard to the cellular telephones, a search is permitted for all records, in whatever form, that constitute evidence, fruits, and/or instrumentalities of drug purchase and distribution.

a. Records of personal or business activities relating to the operation or ownership of the phones (such as user names, passwords, telephone records, notes, books, diaries, and reference materials).

b. Records pertaining to accounts held with companies providing Internet access or remote storage of either data or storage media.

c. Records relating to drugs, drug proceeds, drug distribution, drug importation, money laundering, money transfers, ledgers, contact lists, price sheets, and related documents.

d. Records and information identifying contact information for co-conspirators, communications made in furtherance of the conspiracy, and photographs and videos of co-conspirators.

14. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records of information that is otherwise called for by this warrant (hereinafter, "computer");

a. Evidence of who used, owned, or controlled the computer at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat", instant messaging logs, photographs, and correspondence.

b. Evidence of software that would allow other to control the computer, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software.

c. Evidence of the lack of such malicious software.

d. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the computer.

e. Evidence of the lack of such malicious software.

f. Passwords, encryptions keys, and other access devices that may be necessary to access the computer.

g. Documentation and manuals that may be necessary to access the computer or to conduct a forensic examination of the computer.

h. Records of or information about Internet Protocol addresses used by the computer.

i. Records of or information about the computers Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "Favorite" web pages, search terms that the user entered into any Internet search engine, and records or user typed web addresses.

j. Contextual information necessary to understand the evidence described in this attachment.

Definitions

For the purpose of this warrant:

Computer equipment means any computer hardware, computer software, mobile phone, storage media, and data

Computer hardware means any electronic device capable of data processing (such as a computer, smartphone, mobile phone, or wireless communication device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).

Computer software means any program, program code, information or data stored in any form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.

Storage media means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, or memory card).

Data means all information stored on storage media of any form in any storage format and for any purpose.

A record is any communication, representation, information or data. A "record" may be comprised of letters, numbers, pictures, sounds or symbols.

Return of Seized Computer Equipment

If the owner of the seized computer equipment requests that it be returned, the government will attempt to do so, under the terms set forth below. If, after inspecting the seized computer equipment, the government determines that some or all of this equipment does not contain contraband or the passwords, account information, or personally identifying information of victims, and the original is no longer necessary to retrieve and preserve as evidence, fruits or instrumentalities of a crime, the equipment will be returned within a reasonable time, if the party seeking return will stipulate to a forensic copy authenticity (but not necessarily relevancy or admissibility) for evidentiary purposes.

If computer equipment cannot be returned, agents will make available to the computer system's owner, within a reasonable time period after the execution of the warrant, copies of files that do not contain or constitute contraband; passwords, account information, or personally identifying information of victims; or the fruits or instrumentalities of crime.

For purposes of authentication at trial, the Government is authorized to retain a digital copy of all computer equipment seized pursuant to this warrant for as long as is necessary for authentication purposes.